# 511 Traffic Program
# Enhanced Data Fusion System (EDFS)
# Concept of Operations

**Task Order 6.10, Deliverable 2.2**

**Version 1.0**

*Submitted to:*

**Metropolitan Transportation Commission**
**101 Eighth Street, Oakland, California 94607**

*Submitted by:*

**Science Applications International Corporation**
**1000 Broadway, Suite 680, Oakland, California 94607**

**August 26, 2011**

*Revision Chart*

| Document Description | Date | Version Number |
|---|---|---|
| First Internal Draft | 04/07/2011 | 0.9 |
| First round of MTC's comments incorporated | 04/14/2011 | 0.11 |
| Second round of MTC's comments incorporated | 04/25/2011 | 0.12 |
| IBI's comments incorporated | 05/03/2011 | 0.13 |
| Third round of MTC's comments incorporated | 05/27/2011 | 0.14 |
| Version 1 finalized | 08/26/2011 | 1.0 |

## *Table of Contents*

## *Table of Figures*

# 1 Scope

This document presents the concept of operations for the EDFS replacement enhancement task. For the purposes of this document the replacement for the current "Enhanced Data Fusion System (EDFS)" system will be generally referred to as EDFS for ease of use. This Concept of Operations presents point of view of few stakeholder groups – Traverler's Information Center (TIC) operators and supervisors, MTC staff, TIC managers, systems operations staff, representatives from other regional Transportation Management Centers (TMCs). Specifically, interviews were conducted with peer 511 deployers and stakeholders, e.g. subject matter experts, and were summarized into a report that serves as input to the development of this document. The interviewees are listed as follows:

| Organization | Interviewees |
|---|---|
| Caltrans Headquarter | Mike Jenkinson |
| SACOG 511 | Mark Heiman |
| New York 511 | Todd Westhuis, Rexy William |
| MTC HAO section | Joy Lee |
| LA Metro 511 | Mauro Arteaga, Baron Grey |
| Trans Star (Houston) | John Whaley |
| Florida 511 | Gene Glotzbach |
| Caltrans District 4 | Charlie Price, Hector Garcia |
| ATMS | Sze Lei Leong, Derek Pines |
| IBI Group | Nicholas Day |

## 1.1 Purpose of this Document

This document is divided into the following sections:

**Section 2** presents the EDFS Vision, Goals, and Objectives.

**Section 3** presents the description of the services that will be affected by the EDFS replacement.

**Section 4** describes the changes to the operational and support environment for the new 511 upgrades as part of the 511 EDFS.

**Section 5** presents the risk assessment and impact overview.

**Section 6** presents the assumptions and constraints related to this system replacement effort.

**Section 7** discusses the roles and responsibilities of the various stakeholders**.**

## 1.2 Referenced Documents

A variety of documents are used as references within this report. The list is as follows:

1. SAIC/IBI Group, TIC Operator Manual (Revision V1.0 Final), May 18, 2010.

2. SAIC, 511 Traffic Open Messaging Service Overview (Revision v2.0), April 01, 2010.

# 2 EDFS Vision, Goals and Objectives

## 2.1 EDFS Vision Statement

To provide a uniform solution of collecting static and dynamic events/incidents data from all available data sources, including traffic and transit, provide remote access to the system and provide a standardized means of processing the raw data into meaningful information for distribution into various dissemination channels.

## 2.2 EDFS Goals and Objectives

- Develop an integrated solution for events/incidents information collection, processing, and distribution into a information exchange channel (e.g., Java Messaging System (JMS)) that leads to various information dissemination systems
- Integrate with existing applications that are part of data dissemination system for easier data maintenance and to make the new EDFS the primary event data management tool for TIC operations. The following existing applications will be integrated with the EDFS package: Transit Content Management System (CMS), Traffic Admin Page (including Ticker application for all 511 websites), Congestion OI (including Break-A-Link), 511 Manager, TIC Operations Staff Email (including Caltrans D4 and D5 Emails, CMS Sign Check, Transit Agencies Alerts, and Special Events Notification Email), Emergency Abbreviation System (EAS) for the web and phone, Real Time Transit Hub Sign route messages, Caltrans' Lane Closure System (LCS), CHP Media CAD and Twitter.
- Automate data collection from external sources whenever possible while leaving operators flexibility to approve/edit/reject any automatically collected information or manually enter information whenever needed.
- Improve timeliness and accuracy of the information entered into the EDFS system.
- Improve consistency of information disseminated via all channels
- Reduce the operator labor required for collection, processing and distribution.
- Ensure flexibility for inclusion of potential and existing data sources for events/incidents information
- Ensure access to the system and events/incidents information by different security levels of user groups using various communication methods
- Ensure capability of system reporting and message archival mechanisms
- Ensure web access for all EDFS components is available for TIC operators and MTC staff
- Update the location descriptors and roadways so that all connectors and locations are available to the operators and will work well with dissemination tools
- Ensure system efficiencies to enable faster posting of emergency messaging with the goal of not needing a system administrator to post any emergency message.

# *3* Description of Service

The EDFS is a centralized way of collecting, processing, and packaging event data for dissemination into the desired final destinations. It is described in detail in the following sections.

## 3.1 Data Collection

The system receives incoming data from various sources, which are all considered to be external to the EDFS. They will have different levels of trustworthiness. They may include data coming from EDFS users (TIC operators, MTC staff, etc.), CHP Media CAD XML feed, Caltrans (TMC operators, CWWP, LCS, CMS, etc.), Transit Agencies, Twitter, RSS feeds, the list of trusted sources in the TIC Operators Standard Operating Procedures (SOP) and "non-trusted" events. The frequency of collecting data is either on a regular basis or as needed, depending on the individual data source.

Data from incoming sources may include traffic incidents, planned lane closures, transit service delays or schedule changes, sporting events, severe weather conditions and other information that may be useful to travelers or impact their travel plans.

### 3.1.1 Data workflow states

Each event data feed coming into the system will go through multiple state changes from being a new entry to an archived one. The typical workflow states will be "New", "Discarded", "Published", and "Closed". The workflow state will be changed automatically by the system, depending on the nature of the change (e.g. from "New" to "Published" when operator saves changes and publishes information). The data entries can be moved freely from one state to another, as long as the moves follow approved workflow rules. The workflow rules will be configurable by the system administrators and regulated by the management team. Operators will not be allowed to change the workflow state of a data entry if it violates any of the workflow rules, e.g. changing the state of a data entry from "Published" to "New".

Figure 1 presents the transitions between workflow states.

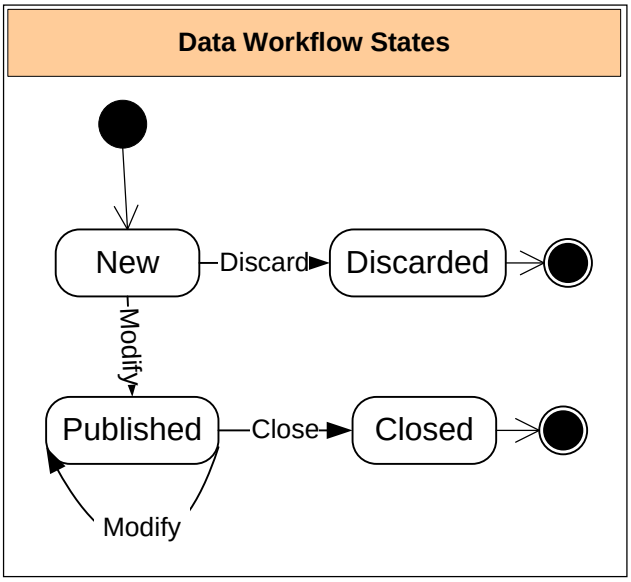


**Figure 1. Data Workflow States in EDFS**

When data is collected from an external data source, it automatically will start as being in a "new" workflow state. Once the operator reviews and/or modifies the new data entry and submits it for publishing, the data entry is said to be in a "published" workflow state. This assumes that the data entry is being published or will be published at some point in the future. Once the operator closes a data entry (which implies that the data entry is no longer being published or is not going to be published), the data entry is said to be in a "closed" workflow state. Operator can close published data entry or discard a new one – close it without publishing.

### 3.1.2 Data Processing

All data sources in EDFS are classified as automated or requiring manual verification, data entry and approval. Data from automated sources will be used to create event records and published automatically without operator interaction, though it can be edited and updated later, by an operator, as with any other event.

Data sources that aren't automatically published are treated as trusted or non-trusted. All data from non-trusted sources require users to review and approve before publishing. Since EDFS users are one of the data sources, the system will categorize the data they entered into trusted and non-trusted categories based on the user group they belong to (data editors, operators, supervisors, administrators, etc.). Data input from TIC operators will be classified as trusted, whereas the data input from some other users (such as transit agencies, etc.) will require additional verification and approval before publishing. Once published, a data entry cannot be edited by a user without having the appropriate privileges/security level. This is to avoid accidental modification or closure of an event in the system.

The system will not auto-publish data entries if minimum required fields are not completed; in these cases an alarm will alert the operator so that the missing fields can be 'filled-in'. Similarly, the system will not allow an operator to manually publish a data entry if the minimum required fields are not completed.

When a data entry is published (by approving a new entry or by saving changes to an existing one), it is sent to JMS and related integrated systems (Transit.511, CMS, Ticker, 511 Manager, etc.) and updated appropriately. Data can be published in advance and will not be disseminated until the specified activation date/time. After the specified publishing period is over, the data entry will be closed automatically, presenting a reminder to the users at a predefined time before closure. Data entry also can be closed manually using data editing functionality. Users will be able to edit or close entries regardless of their publishing status. Edits to entries will be published for the dissemination system to pick up and update its own records accordingly. Closed entries will stay in the system for predefined time (e.g. 10 days) for further reuse or re-publishing if needed.

After 10 days, closed data entries that have not been modified recently will be automatically archived. Published data entries that have not been modified recently will also be automatically archived after a predefined period of time (e.g. 2 days). New data entries that have not been published after a predefined period of time (e.g. 2 days) will be automatically closed and archived.

In addition to publishing, data will be fused from multiple sources and updated as needed. Automatically published data sources will be monitored to identify relevant updates for other actively published data entries. Information in the system will be updated and republished automatically to ensure it is always up to date. For non-automatic data sources, i.e. data sources that cannot be published automatically, EDFS will warn operators whenever new updates become available and suggest selection of published data entries for update. Data coming from multiple data sources may be used to update a particular published data entry as long as EDFS is able to match the data entries in multiple systems.

Figure 2a presents the lifecycle flow chart of data entries in EDFS.

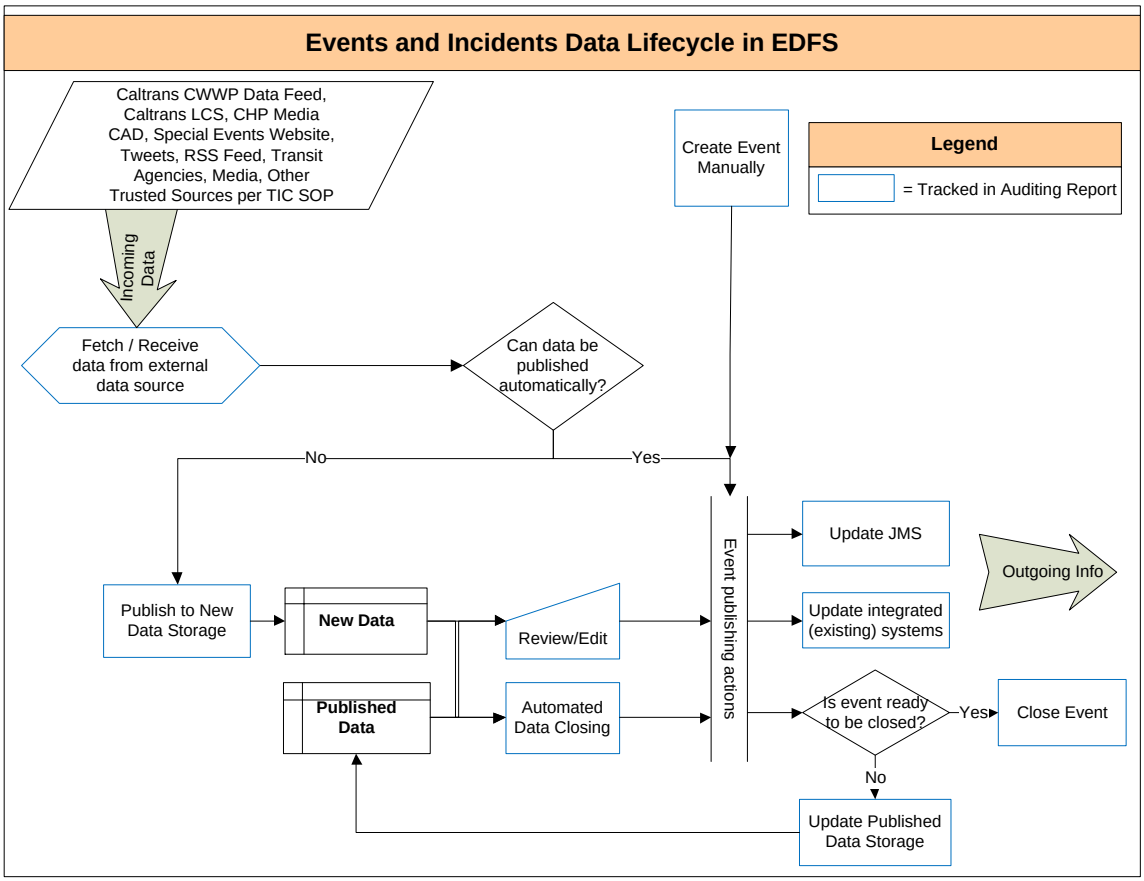


**Figure 2a. Lifecycle Flowchart of Data Entries in EDFS**

Figure 2b presents the manual workflow of reviewing and editing the data entries in details.

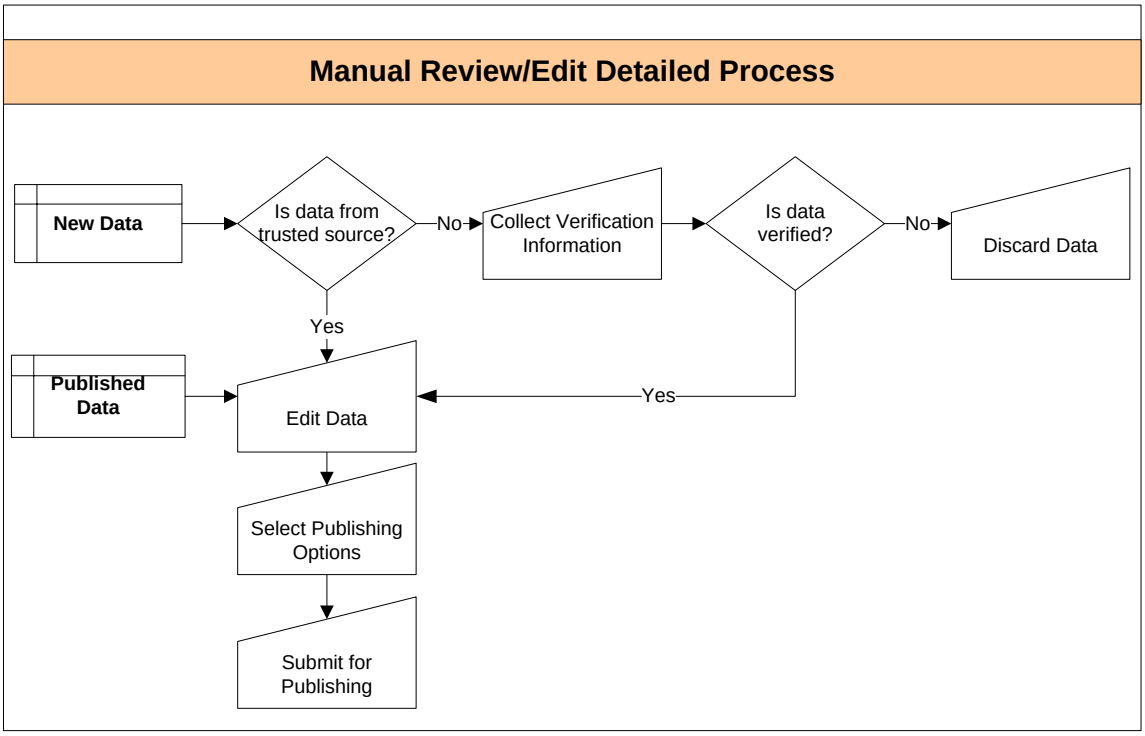


**Figure 2b. Manual Review/Edit Detailed Process Flow Chart**

### 3.1.3 Reviewing Existing Data Entries

Users will be able to view a sorted list of existing data entries on the EDFS Data List Interface. An existing data entry is a data entry that is new, published recently, or closed recently, e.g. in the past ten days. Published data entries will always remain in the existing list of data entries regardless of whether it has been recently modified or not.

The data entry list will use visual aids, such as color-coded icons, font types and styles, and have sorting and filtering options to help users quickly identify data entries by their characteristics. For example, users can easily identify SigAlerts if they were marked as red in the data entry list. For each data entry on the list, users will be able to view the source of the event, the content, time properties, and relevant details of data entry. The length of the list of data entries will be reasonably defined to optimize the balance between coverage and usability.

If there were two separate data entries that refer to the same incident/event, users will recognize the relationship between the two based on their knowledge of the situation and frequent interaction with the list of existing data entries. They will also be able to recognize the relationship by using the map interface to visually identify events that are closely located with each other. They may update either one of the data entries and close the other one to avoid duplication of the same incident/event in the system. Whenever possible the system will identify related events that are already in the system and suggest it to operator for update. In cases when a data source has updated information for a particular event or incident, the information will enter EDFS as an update to the corresponding data entry in the system. Relationship between events will be established for tracking and reviewing purposes.

### 3.1.4 Monitoring Existing Data Entries

The system will send an alarm to the user that a data entry requires user intervention or immediate attention, e.g., an incident is expiring in the next five minutes or a SigAlert has been issued. The alarms will either be pre-defined by the users when they modify a data entry or by the system, depending on the type of data. For example, the system will send users an alarm 30 minutes prior to publishing a planned special event data entry. Users will confirm if it is going to take place. Also, when a published data entry has not been modified in a long time, the system will bring it to the users' attention through system alarms.

Users will be able to acknowledge the alarm or snooze the alarm. Acknowledging it will prevent the alarm from displaying again. Snoozing the alarm will temporarily disable it, but it will be displayed again after a short while, e.g., three minutes.

### 3.1.5 Processing of an Existing Data Entry or Entering a New Data Entry

#### *Modifying the Information*

Modification of data entries may be made manually by the users and/or automatically by the data sources, including the description of an incident, the duration of a planned road construction, the level of trust of the data source, the start time of an alarm, the change of priority of a data entry, and others.

When new data enters EDFS, the individual data sources, whether from a trusted or non-trusted source, will pre-fill the data entry forms on the EDFS Data Details Interface. Users will be able to modify any information in each of the data entry forms. Modifications will be performed with limited free text input. This will be done with the assistance of drop down menus and check boxes in order to minimize response time and to control messaging. Modifications include defining the descriptions of the published data, the data source, the dissemination channels to be used, and any relevant details in a data entry.

All information defined in the data entry forms will be modifiable at any time as long as the data exists in EDFS. For example, in cases where the event information initially entered by the system (using data received from data sources) is insufficient or inaccurate, users will be able to modify it. Also, in cases where the suggested dissemination channels are insufficient or inaccurate, the users will be able to modify the choices until all relevant channels have been selected. Another example is that before confirming that a data entry is ready for publishing, users will always have the ability to revise any information defined in the data entry form.

If new data originated from a trusted source, its state will change from new to published if the new data is either ready for publishing at the specified publishing date and time, or if it has already been published automatically.

#### *Defining Location*

The EDFS will have tools that assist users to geo-locate the information accurately, such as the use of a map interface to accurately pinpoint an incident location. Since different data sources have different means of describing a location, the EDFS will convert them into a common location format (latitude/longitude) automatically whenever possible. Whenever a conversion of a location into lat/long coordinates is not possible, it will pre-fill the data entry form with the original descriptions that come from the corresponding data source. Original descriptions may include landmarks, post-miles, freeway exit names, and others as defined in the EDFS Requirements Specification Document. Location description for data dissemination will be defined in addition to latitude/longitude information using landmark names, cross streets, exit names, and postmiles that can be cross-referenced on a map interface.

The location of an event is necessary for the system to formulate an event description for publishing. When event location is not available or is insufficient for the system to define the exact location of the event, operators should follow the defined procedures in SOPs to provide an appropriate description for the event location. Operators can also make use of the map interface to identify the exact location description based on the limited information provided by the data source(s).

### *Defining the Dissemination Channels*

During the process where users modify a data entry, they will also be able to select appropriate dissemination channels on the EDFS Data Details Interface. The system will provide the users with the ability to select available dissemination channels to publish the information and appropriate tools to activate. Examples include: 511.org, individual 511 modal web pages, 511 phone, ticker and social network interfaces. While the options can be manually selected, the system will also suggest final dissemination channel(s) to the users. The suggestions will be based on the assumption that certain types of data have a set of typical final dissemination channels.

*Note: EDFS will be built with extensibility in mind so new dissemination channels and publishing options can be added later as extensions.*

### *Publishing Data*

Users will be able to specify the publishing properties of a data entry. The properties may be the duration of disseminating the data (activation/deactivation date and time), its relation to another data entry, and its priority among all disseminated data if applicable. The user has the final decision on verifying the readiness for publishing the event. Users will be able to instruct EDFS to publish a data entry as long as the minimum system requirements have been met. A list of minimum requirements will be recorded separately in the EDFS Requirements Specification Document. After these properties are specified, the user will be able to publish (or re-publish) data and make appropriate changes in external integrated systems.

### *Data ownership*

When a traffic incident data entry is new, it will appear in the EDFS Data List Interface and will be marked as “not-owned” (ownership is not applicable to other types of the events). Users will be able to open the entry for viewing and/or modifying the details. At the point where the user saves any modifications made to the details, the incident data entry is said to be “owned” by the user. The incident data entry will then be marked as “owned” in the EDFS Data List Interface. At the same time ownership doesn’t prevent other operators in the system from making changes to any of the incidents - it is a flag that somebody is tracking this particular incident and making sure all updates are applied as quickly as possible. If an incident is not owned by any of the operators it means that either it is new and no one has reviewed it yet, it is very low priority data coming from non-trusted source or the operator who was monitoring how that incident evolves and making changes as necessary logged off the system. In latter case some other operator will make changes to it as new updates come in and will become owner of the incident automatically.

In general, defining the ownership of incidents will help users, including both the system and the operators, to closely communicate with each other and thereby manage incidents more effectively, especially in cases of emergencies where operators cannot work at the same location. This increased communication between the users will not only help to avoid redundant efforts in managing a particular incident, but will also allow users to focus their attention on managing their list of incidents in a more controlled manner.

As the owner of the incident, the user will be responsible for updating the incident and tracking any incoming updates for the particular incident. The system will remind the owner (for example, in the form of system alarms) to revisit and modify the incident when the incident has an update from its data source. The system will also remind users if related incidents owned by other operators received an update. The owner will then be able to view and/or modify the incident he/she currently owns or the related incidents that were mentioned in the alarms if appropriate.

It is important to note that every user who is logged into the EDFS can perform any operators’ actions to any incidents, such as viewing, modifying, discarding, or closing the incident. The last operator to perform actions on the incident will be considered to be the owner of the incident.

The owner will have the responsibility of managing the incident until he/she logs off from the system. In cases where the incident has not been closed before the user logs off from the system, the incident will become “not-owned” again. Note that changes in ownership will be continually tracked as part of the audit tracking process.

Apart from operators, the system will also be considered as the owner of events in certain situations. For example, events that are published automatically will be owned by the system. In this case, the system will be responsible for viewing, modifying, and closing the event. These events will follow the same ownership rules as described above.

*Note: TIC SOPs will have to be updated to address ownership and responsibilities related to owning the incident.*

## 3.2 Data Dissemination

Various data sources may have different publishing options – some of the trusted sources may be configured as published automatically, etc. Figure 3 lists examples of publishing options for trusted and non-trusted data sources.

| | Trusted Data Sources | Non-Trusted Data Sources |
|---|---|---|
| **Automatically Published** | **Examples:**<br>LCS 10-97 and 10-98 messages. | × |
| **Manually Published** | **Examples:**<br>CHP CAD, MTC Staff Call, Emails from Caltrans and transit agency partners | **Examples:**<br>Call from the public, Twitter Account, Email. |

**Figure 3. Publishing Options for EDFS Data Sources**

When the data is ready for publishing, the system will publish the data in two ways.

In the first way, the system will publish data indirectly to the final dissemination channel(s) through the messaging system, JMS. The JMS is a system that is separate from the EDFS system and will propagate ("push") data towards their final channel(s) for dissemination.

In the second way, the system will publish data by directly publishing them to other final dissemination channel(s) that are not using JMS for data exchange. There will be direct communication between the EDFS system and these final channels. Examples of direct publishing channels are the ticker on 511 web pages, the Transit CMS, 511 Manager, Congestion OI, social networking sites, and others as defined in the EDFS Requirements Specification Document.

Selection of the dissemination channels to be used will either be pre-configured for data sources that are eligible for automatic publishing or be manually determined and approved by operators for non-automatic data sources.

The EDFS system will include the function of monitoring the process of publishing data into the JMS and dissemination channels that provide appropriate APIs (for example, the ability to provide a list of all published incidents). Messages will be sent to a predefined list of recipients in cases when the list of published data entries in EDFS doesn't match data in any of the dissemination systems or JMS. In this way, system administrator will be notified when there are discrepancies between data in JMS, Interactive Voice Response (IVR) or web systems and will start investigating the cause for the discrepancy.

## 3.3 Auditing

Data entries in the EDFS will be audited throughout their entire lifecycle. Each action including data changes, publishing, closure, etc. will be recorded along with date/time stamps and user (who performed action) identification information, such as user name.

### 3.3.1 Audit Reporting Mechanism

At the initial point when data enters the system, an audit reporting mechanism will begin tracking any modifications made to each data entry throughout their lifecycles. Modifications will be tracked until it reaches a state where no further operations or actions are expected to be taken (e.g. the entry is closed).

In addition to workflow states, the auditing report mechanism will be capable of continually tracking any modifications made to the data entries, as discussed in Section 3.2 Data Processing. The auditing report mechanism will report information related to each modification, such as the timestamp, the username, etc. to maximize potential benefit of the reports.

Along with data changes auditing mechanism will keep tracking of alerts and reaction to them - for example alert message for incident owner, then, when owner is not capable to update incident with new data, alert to the other operators logged in.

### 3.3.2 Auditing Report

All modifications made to the data entries will be saved into an ongoing record known as the Auditing Report. The Auditing Report consists of changes made to each data entry collected in real time, from the most recent changes to the changes made in the past number of days. The number of days in the past will be configurable by the system administrators and regulated by the management team.

Authorized user groups will be able to view the Auditing Report at any time. They will be able to sort and filter the Auditing Report within the EDFS to show records they are most interested in viewing, such as filtering the records by a specific username or a certain timeframe.

If the user requested a report that contains information on the current date, the report should refresh automatically to accurately reflect the real-time information as needed. In this way, the user can view the latest version of the report as the changes to the contents are made.

Users will be able to export the Auditing Report out of the EDFS in Adobe PDF or Microsoft Excel formats.

## 3.4 System Maintenance

The system will have the flexibility to incorporate static and dynamic data updates to maintain the accuracy of publishing the data into various dissemination channels. For example, the system will incorporate basemap updates as needed. The system will also be able to allow updates to the drop down menu selections. Authorized user groups, such as the system administrators, will be able to manually update the drop down menu selections as needed.

The EDFS system will have automatic and redundant failover properties using multiple servers running in parallel (i.e., a load balanced cluster). The system will be able to track all system issues and failures and use them as reference for troubleshooting activities in the form of system logs. EDFS will also provide APIs for system state reporting to be used by external monitoring tools.

The system will be scalable to support potential expansion of dissemination destinations. The system will also be scalable to expand or reduce the potential data sources as needed. System administrators will be able to configure the system into collecting data from new sources that are not currently connected with the system.

Finally, the system will be capable of adding or removing individual users and/or user groups. System administrators will be able to manage the list of users, including the access level, creating and closing user accounts, and other user account issues as appropriate.

# *4* Operational Scenarios

This section contains high-level descriptions of the most common scenarios associated with the use of EDFS. For this document, a scenario is presented as a step-by-step description of how EDFS should operate and interact with its users and its external interfaces under a given set of circumstances. The scenarios contained in this document do not represent the full set of scenarios that exist for EDFS – for example it does not include scenario for automated data publishing. Additional scenarios and further details of the scenarios contained in this document will be developed as part of the detailed design task and documented in the System Design Document. The Unified Modeling Language (UML) will be used to document the details of the scenarios. Actors in the UML represent user roles in the system that have been assigned to physical users– for example the same system user or MTC staff member may play system administrator, supervisor and operator roles at once and have access to the functionalities described in the scenarios. EDFS modules may play roles as well - for example data collection module that is configured to publish data automatically would be playing role of operator in new data entry publishing process.

For this section, the scenarios have been grouped into three categories: user scenarios, management team scenarios, and system administrator scenarios. User scenarios describe activities that the system will perform based on interaction with an operation staff. Management team scenarios describe activities that the system will perform based on interaction with a management staff. System administrator scenarios describe activities that the system will perform based on the interaction with a system administrator.

It is important to note that various organizational roles can perform as either one of the actors in the following operational scenarios.

## 4.1 Operators

The following sections provide some operational scenarios for the Operators.

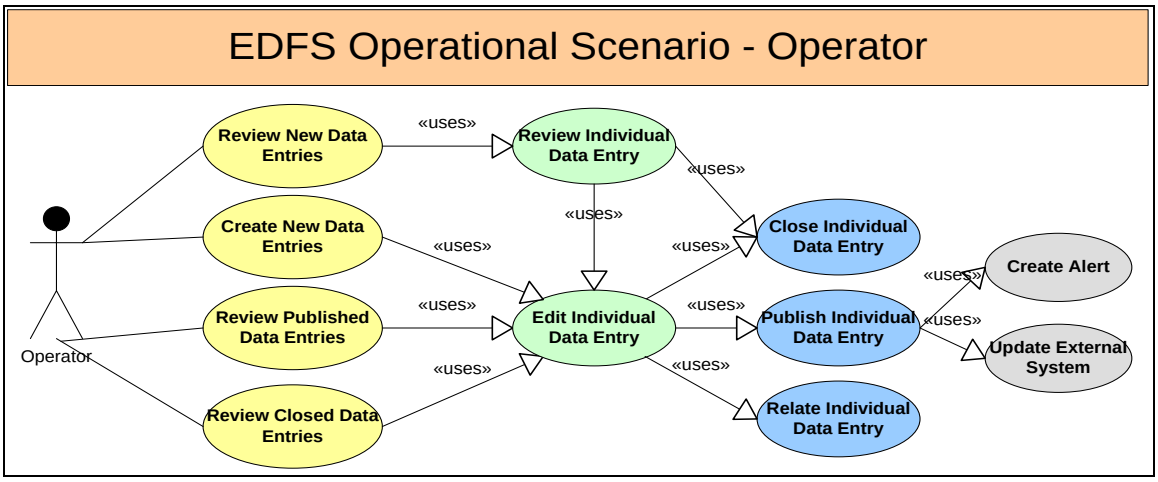


**Figure 4. EDFS Operational Scenarios - Operator**

### 4.1.1 Review and Modify Incoming New Data

*Respond to Data from a Trusted Source*

*Scenario 1:* An operator logs into the EDFS system using his user account log-in information. He can then review the incoming events/incidents data. He selects the details of one incident, and observes that the incident originated from a trusted data source, e.g., CHP Media CAD. He is able to see the location of the incident on the map interface in EDFS. He then modifies the incident data in the event description that was generated automatically by the system to make it suitable for the public dissemination. He then selects the 511 Traffic map, ticker, and 511 Phone along with the specified phone menu locations to publish the information. After publishing the information, he confirms that the information was published successfully out of the EDFS by manually checking all of the chosen dissemination channels. He also confirms that incident record was added to the list of published incidents in EDFS.

*Respond to Data from a Non-trusted Source*

***Verify Trustworthiness of a New Data Entry***

*Scenario 2:* An operator logs into EDFS system using his user account log-in information. He reviews the incoming events/incidents data. He selects the details of one event/incident, and notices that the event/incident is flagged by the system as originated from a non-trusted data source, e.g. Friends of 511. Operator then verifies the trustworthiness of data by searching for a similar event/incident mentioned by the news on the radio, CHP CAD, TMC, and Caltrans D4 messages, or by direct observation via Caltrans camera feed. He is able to identify a similar event/incident from the news on a radio station, so the operations staff follows the procedures to review, modify, and publish the event/incident as described above.

***Verify Trustworthiness of a Special Event that was posted on Twitter***

*Scenario 3:* An operator logs into EDFS system using his user account log-in information. He received a Tweet saying that a concert is planned to happen next month in San Francisco. He verifies with an official website and obtains the details of the planned concert. He then creates a new data entry in the EDFS and enters the relevant information about potential traffic impact. He then defines the start time of the alarm to remind operators of this planned event again when the event's activation date and time approaches.

#### *Response to Data that Affects Integrated Systems*

*Scenario 4:* An operator logs into EDFS system using his user account log-in information. As he reviews the incoming new events/incidents data, he evaluates the severity level of the event/incident and determines that the severity of event/incident affects the way of processing information in other systems. Particularly, the incident was causing closure of all lanes on I-80 in both directions. He reviews and edits the data into useful information as described in the scenario "Responding to data from a Trusted Source". Additionally, he selects the options to activate Congestion OI, Event OI, prepares and uploads into EDFS an emergency floodgate message to be published via 511 Manager. He then publishes the event/incident as mentioned in the scenario "Respond to Data from a Trusted Source".

#### *Operating in an Emergency Situation*

*Scenario 5:* Due to an emergency situation, the 511 Traveler Information Center is closed. From his home or other location, an operator logs into the EDFS system using his user account log-in information using his computer. He is able to perform normal operations on the EDFS system remotely via web based interface.

### 4.1.2 Review and Modify Manually-Created New Data

*Scenario 6:* An operator logs into EDFS system using his user account log-in information. He receives a phone call from a MTC staff, and is informed of an incident on a major freeway in the SF Bay Area. The operator then obtains all relevant details about the incident and inputs the details, including the time and date, the name of the MTC staff member providing the data, the incident descriptions, and other details into the system as part of the process in creating a new event/incident. He saves the data and is able to see it in the list of published incidents. He then reviews, modifies, and publishes the information as/when needed by following the procedures mentioned in the scenario "Respond to Data from a Trusted Source".

### 4.1.3 Review and Modify Published and Closed Data with the Aid of Alarms

#### *Re-Open a Closed Data Entry*

*Scenario 7:* An operator logs into EDFS system using his user account log-in information. He opens the EDFS Data List Interface and filters the list to show only the closed data entries. He decides to re-open one of the closed events based on a recent notice of the event's extended

timeframe. When he re-opens it, he is able to edit the information in the EDFS Data Details Interface, in the same interface where operators modify published events. He modifies the event by extending its duration, reviews the modifications and other details of the event, and publishes the updated event by following the procedures mentioned in the scenario "Respond to Data from a Trusted Source".

### *Update a Published Data Entry*

***Manually Recognizing the Relationship between New Data and Published Data***

*Scenario 8:* An operator logs into the EDFS system using his user account log-in information. He has been reviewing and modifying data entries for a while. As he was reviewing an incoming new CHP incident, he recognizes that it is an update to a published road closure event that was reported by Caltrans and was not brought to his attention by the system automatically. Particularly, the update is the re-opening of a freeway in one direction from a previous closure in both directions. He then relates this new data entry to the published data entry in the system. The system will indicate that the two data entries are related (based on external data source identification information) and suggest operator to establish relationship between them. Operator accepts suggestion and relationship gets established. He verifies that the new CHP incident information is accurate and decides to modify the description in the newer data entry to indicate the re-opening of a freeway in one direction. He does not want to modify the older data entry because it will take more effort to update it to incorporate the new information received. He reviews the modifications and other details of the road closure event, and publishes the road closure event data by following the procedures mentioned in the scenario "Respond to Data from a Trusted Source". The system warns the operator that there is a related data entry to the one that is being published and advises the operator to verify that the same incident is not being actively published more than once. The operator views the related data entry, i.e. the actively published Caltrans road closure event, and closes it because it is outdated and will not be used anymore.

***Automatically Recognizing the Relationship between New Data and Published Data***

*Scenario 9:* An operator logs into the EDFS system using his user account log-in information. He opens the reviewing screen to review all events/incidents data entries. He notices that one of the published CHP Media CAD incidents has a recent update from CHP. Particularly, the incident is now blocking the right lane on a major freeway, rather than two right lanes. Operations staff looks at the CHP incident ID number and confirms that the system has accurately related the new incident data entry to the published data entry. He then modifies (if needed) and re-publishes the updated description to the dissemination channel(s) by following the procedures mentioned in the scenario "Respond to Data from a Trusted Source".

*Note: This scenario is applicable for non-automated publishing only. Data sources configured for automated information publishing will recognize relationships and update data automatically.*

### *Confirm Closure of a Published Data Entry*

*Scenario 10:* An operator logs into the EDFS system using his user account log-in information. As he was reviewing the list of all data entries, an alarm on the screen drew his attention. He reviews the alarm, which reminded him that one of the published incidents is about to close in the next five minutes. Since no relevant updates to the incident are needed, he confirms that the incident does not need to be extended or updated and can be closed. He confirms the alarm and continues reviewing the list of all data entries. After five minutes, he filters the list so that only the closed data entries display. He is able to identify that particular incident in the filtered list.

## 4.2 Management Team

The following sections provide some Operational scenarios for the Management Team.

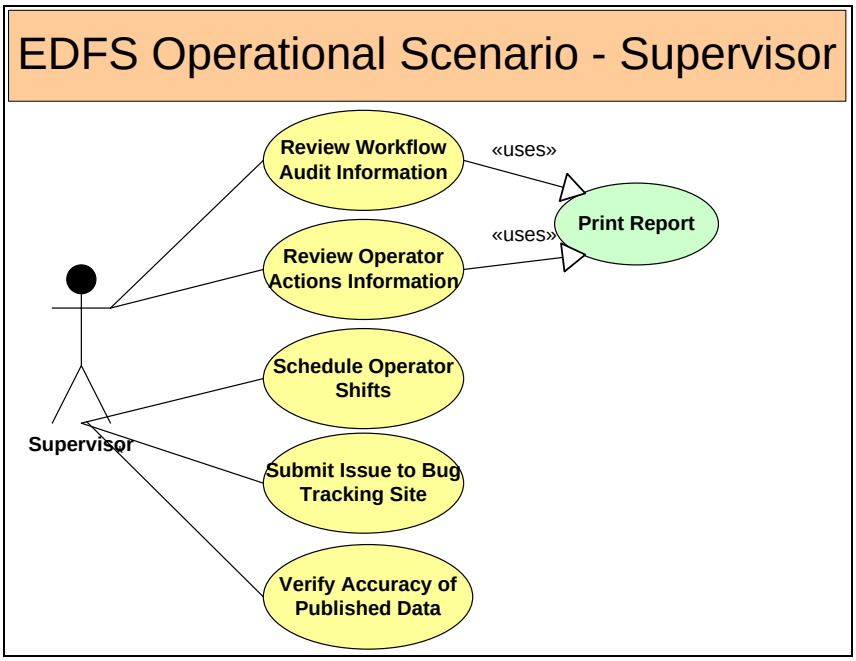


Figure 5. EDFS Operational Scenario - Supervisor

### 4.2.1 Obtain Archived Data Entries

*Scenario 11:* A supervisor logs into the EDFS system using her user account log-in information from her office. She chooses to access the pool of archived events/incidents and particularly wishes to obtain the details about a particular incident on CA-237 W that happened last week, January 4, 2012. She then filters the pool of events/incidents to show only the incidents that were published out of the EDFS system on that day. In the pool of incidents, she finds the incidents associated with the freeway by specifying the name of the freeway, i.e. CA-237 W. She then is able to view all four archived events/incidents that occurred on January 4, 2012 along CA-237 W. After identifying the incident of interest, she observes the historical series of actions

taken and the original information that has been published for this incident. She is then able to print a summary report of the information for further review.

### 4.2.2 Obtain Auditing Report

*Scenario 12:* A supervisor logs into the EDFS system using his user account log-in information. He chooses to access the list of EDFS data entries. He wishes to obtain the name of the operator who is aware of the series of breaking news messages that have been and/or are currently displayed on the 511 website. He enters appropriate keywords in the search field in order to identify the messages that are related to the incident. He is then able to observe the audit details related to the message and identify the operator that has modified and is modifying the messages. He then contacts operator about the breaking news messages.

During a call with the operations staff, the supervisor and the operator both determined that one of the messages is outdated and should not continue to be displayed on the 511 website. The operator closes the message and the supervisor verifies that the relevant entry has been changed to "Closed" in the audit report. He also noted that the operator name, the time of the closure, the reason for closing the incident, and other relevant details appear in the report.

### 4.2.3 Obtain Customized Report for a Selection of Data Entries

*Scenario 13:* A MTC 511 staff member logs into the EDFS system from his office computer using his user account log-in information. Today is July 1, 2012 and he wishes to obtain a report that would help to summarize the average time needed in June to distribute an event/incident from a trusted data source. He specifies the criteria of the report: the beginning and ending date, e.g. June 1 and June 30, and the data source type, e.g. SAIC employee. He obtains the report and is able to observe all the details about the events/incidents matching these criteria, such as the names of the operators, the status of the events/incidents, the published content of the event/incident, etc. He then specifies that he is only interested in the times of entry and publishing in addition to the names of the operator(s). The new report now contains the information he needs, which he can then print for further analysis and/or save as an excel file or a pdf file.

He now wants to find events/incidents in the report that are related to the 45-min. BART major service delay that happened in June. He is able to search the newly created report by specifying the keywords "BART delay". He is then able to identify all events/incidents related to BART delay and find the entry for that particular 45-min. BART delay incident.

## 4.3 System Administrators

The following sections provide some operational scenarios for the System Administrators.

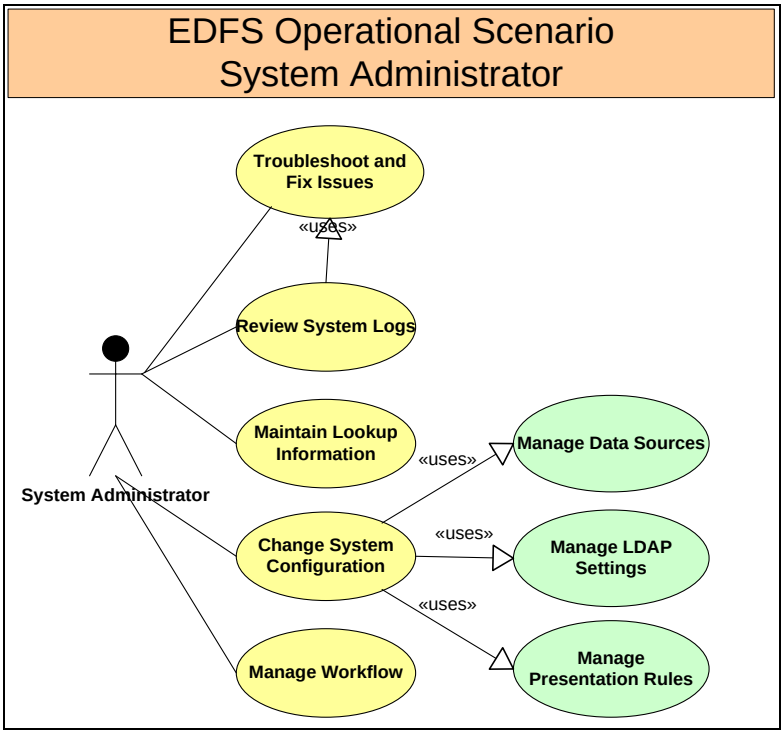


**Figure 6. EDFS Operational Scenario - System Administrator**

### 4.3.1 Modify System Information to Perform Regular Maintenance Activity

*Modify System When Updates to the Defined User Selections are received*

*Scenario 14:* A system administrator is notified that new data for the lookup lists of landmarks and new base map information are available. The system administrator logs into the EDFS using his administrator log in information. He views the list of configuration settings and adds the new landmarks to the landmarks dataset. Once he made that change in EDFS, he saves the change and verifies that the new landmarks are made available in the appropriate places in EDFS. He then looks at the backend procedures and configures the basemap updates. Once he made the configurations, he executes the updated procedures to apply those changes. EDFS system generates change report to be used during next recording session by IVR system maintenance team. He performs a series of testing to verify that the system is running smoothly. He finds out that the system is indeed functioning properly.

*Maintain User Groups and Access Levels*

*Scenario 15*: A system administrator is notified that the TIC operators now should have access to the functionality of generating audit report. He logs in to EDFS using his log in information and updates the user group settings and privileges. He then saves the changes and checks that the TIC operators now have the privilege to generate reports. He then reviews the list of user accounts and notices that one of the user accounts is no longer in use. After he verifies the user account is appropriate to be removed, he removes the user account from EDFS. He also reviews the appropriate documentation and updates it as needed.

### 4.3.2 Modify System when Additional Data Source is Available for Integration

*Scenario 16:* A system administrator is notified that a new data source has to be integrated. He looks at the backend procedures, determines that there is no need to custom code development as such data source is already supported and modifies the system configuration in order to add the new data source as one of the EDFS data sources. The system administrator runs a series of acceptance tests to verify that the system accepts incoming event/incident data from the new data source and that the impacts, if any, to other systems. He confirms that the system is functioning properly, including archiving of the new data source, and updates documentation as needed.

### 4.3.3 Respond to System Notifications of Error Messages

#### *Notification of Partial or No Data Received from Data Source(s)*

*Scenario 17:* As part of the regular system monitoring activities, a system administrator checks to see if he received any system error messages. He finds out that an error message is received, saying that there is no communication between Twitter, an EDFS data source, and the EDFS. He follows troubleshooting instructions to determine where the problem is. Particularly, he ensures the receiving systems are operational and checks the log files to determine if any error conditions were detected. He then checks the other data sources to ensure they are active, the status of network connectivity and firewall settings. He also coordinates with the operations team to determine if any recent changes could have caused the issues. At the same time, he coordinates with the data source provider to ensure they are operational. He identifies the issue to be related a recent change to the firewall configuration. He submits firewall configuration change requests, gets confirmation that it was updated and runs a series of tests to ensure that Twitter feeds are now entering EDFS as expected.

#### *Notification of Partial or No Response to Information Publishing Request(s)*

***Error notification of Partial or No Response to Messaging Server Leading Towards the Final Dissemination Channel(s)***

*Scenario 18:* A system administrator receives a notification that there is no communication or partial communication between the EDFS System and the messaging server (JMS). He performs a troubleshooting similar to the steps when the system administrator receives notification of partial or no data received from EDFS data sources. In addition to these steps, he checks if the web dissemination team has made any recent changes that would have caused the issues and checks the logs of the messaging server for possible problems. After identifying cause of the issue, which happens to be related to a recent software update made by the software vendor, he contacts the software vendor for a support. After receiving update instructions he changes configuration and runs a series of tests to ensure that Twitter feeds are now entering EDFS as expected.

***Error Notification of Partial or No Response to Direct Dissemination Channels***

*Scenario 19:* A system administrator receives a notification that there is limited communication between the EDFS System and the direct dissemination channels. He follows troubleshooting instructions similar to the steps when the system administrator receives notification of partial or no data received from data sources. In addition to these steps, he checks the logs of the dissemination systems for possible problems. After identifying the cause of the issue, which happens to be related to a recent configuration update made to the Ticker application, he coordinates with the appropriate parties to fix the issue and runs a series of tests to ensure that data is now entering disseminated as expected.

### *Notification of Internal System Errors*

*Scenario 20:* A system administrator receives a notification that the system is experiencing internal errors. He carefully reads the notification to find out what the internal error was related to; such as one of the EDFS servers going down, the databases rejecting recent configuration changes, or another internal system issue. After identifying that one of the EDFS servers' Network Interface Card is not functioning properly he determines a solution to correct the issue and contacts hardware providers and vendors for support. He also logs into EDFS using his log in information and makes necessary configuration changes to the network settings to fix the issue. After saving the changes and executing updated backend procedures, he runs a series of tests to ensure that the EDFS is functioning properly again and confirms that he receives no further system error notifications.

# *5* Assessment of Impacts

This section describes the operational and organizational impacts of the proposed EDFS replacement on the users, the developers, and the support and maintenance organizations. It also describes the temporary impacts on users, developers, and the support and maintenance organizations during the period of time when the new enhancement is being developed and installed.

This information is provided in order to allow all affected organizations to prepare for the changes that will be brought about by the new enhancement and to allow for planning of the impacts on the user groups and the support and maintenance organizations during the development of, and transition to the new enhancement.

## 5.1 Operational Impacts

It is anticipated that the EDFS system will be fully integrated with the other 511 systems. Any new servers would reside on the same Local Area Networks (LANs) as the existing systems, and would thus be managed by the same system administrators that manage the rest of the 511 systems. Depending on the volume of data sent/received by the EDFS, additional bandwidth may be required, although it appears to be unlikely. Regardless, the same internet and/or Virtual Private Network (VPN) connections would be managed by the operational staff. As EDFS represents a replacement of the existing system the overall number of new partners and

stakeholders would be relatively low. This level of change would not require new staff; although additional troubleshooting procedures may have to be implemented depending on the types of issues encountered in supporting the new EDFS and expected support from the partners and/or software vendors.

TIC operations will be anticipated to have lower staffing levels when the EDFS replacement system is in place, largely due to the automation and increased flexibility of inputting data into the EDFS replacement. TIC operations staff and MTC staff will have the flexibility of dealing with emergencies as the new EDFS is anticipated to be a customized and a highly accessible web-based solution. TIC operations staff will also be experiencing increased levels of evaluation on their performance due to the availability of automated tracking of their actions in the EDFS. These tracking records are expected to form the basis of one of the ongoing performance metrics of the TIC operations.

Increased stability will be another impact on TIC daily operations. The new EDFS will require a decreased number of system restarts so that TIC operations staff would have a stable system to use. Changes in monitoring systems are also anticipated to help stabilize the system. It is expected that retiring the framework and old EDFS servers would help reduce the frequency of system errors and/or failure associated with old hardware and software systems.

Training of the operators will be needed as part of the new system introduction. SOPs and Emergency Operations Plans (EOPs) will need to be updated to reflect changes in the functionality and ability of the TIC and MTC staff to access EDFS remotely via web-based interface. A transition period will have to be planned as part of new system deployment plan.

## 5.2 Organizational Impacts

The organizational impacts associated with the EDFS replacement are related to the operations and maintenance of data input and data providers. Additional responsibilities that will have to be specified include the level of MTC's involvement in the operator's environment since they will have direct access to the new EDFS interface. There will also be increased channels of communication between MTC and outside organizations such as Caltrans and CHP as they become the data providers, i.e. the data sources in the new EDFS. It can also be expected that the number of operators in the TIC will decrease due to the increased level of automation.

## 5.3 Impacts During Development

The impacts during development will be determined by the proposed development approach. Depending on the buy vs. build approach, there will be different levels of impact during development and systems transition. TIC operations should not be affected until the new EDFS is fully in place and thoroughly tested as being fully operational. The development and initial configuration of the new EDFS should not impact operators and should have minimal impact on systems maintenance staff.

# 6 Assumptions and Constraints

The following is a list of high level assumptions and constraints that have been retained when describing EDFS replacement system concept of operations (and requirements):

1. All data entry functions that current EDFS system currently provides shall be preserved (alerts, drop-down list based entry, etc.).
2. Multiple users (at least 20-30) shall be able to work (review/edit/publish data) in parallel without negatively affecting each other's work results or system performance.
3. New system shall have web-based user interface for data entry that doesn't require additional plug-ins, players, etc. and runs without functionality degradation on all major web browsers (Firefox, Internet Explorer, Chrome, Safari). It shall use application and database servers for all data processing and storage needs.
4. New system shall integrate with existing data exchange system (JMS) and shall not require development on data exchange system level, i.e., it shall use existing data formats, APIs, etc.
5. New system shall integrate with existing systems (511 Manager, Congestion OI, Transit CMS, Ticker, etc.) and publish data or make configuration changes using existing APIs. Documentation for the APIs shall be available or developed as needed. Missing integration APIs may need to be developed.
6. The new system shall be able to incorporate data feeds from CHP (Media CAD) and Caltrans (Commercial Wholesale Web Portal, Lane Closure System).
7. Development and deployment of the new EDFS system shall not require any changes in other/existing parts of the 511.
8. Existing EDFS system shall be able to run in parallel with the new one during development, installation, training, switchover, etc.
9. New system shall have built-in failover, redundancy and scalability mechanisms along with error reporting, event tracking and messaging.
10. New system shall not require proprietary hardware or software to be installed except for EDFS system itself and operating system.
11. New EDFS system shall be able to receive data from external data sources using existing protocols/channels/formats. Adding new data sources shall not require additional development if format/protocol is already used by the system and would be implemented as system configuration change task by the system administrator.
12. New EDFS system user authentication/authorization/access control mechanisms shall be flexible enough to provide fine-grained access control and shall integrate with industry-standard solutions used by 511 (Lightweight Directory Access Portal).

# 7 Roles and Responsibilities

MTC is the lead agency responsible for the overall coordination of the EDFS architecture and implementation including the oversight of the integration of the real-time data received from the partner agencies with the 511 and 511.org systems. Integration of the real-time data from the partner agencies will include receiving the real-time data in the format defined under the

architecture and appropriately routing it through the 511 system for ultimate dissemination via various 511 channels. The roles and responsibilities of the partner agencies include providing real-time incident/event data for free and in a standard format defined under the architecture to the 511 system.

The following table lists additional details for each identified role in the EDFS project.

| Agency/Partners/Contractors | Roles and Responsibilities |
|---|---|
| MTC | Overall Coordination<br>Setting Project Priorities<br>Document Review and Approval<br>Test Readiness Approval<br>Lead of Change Control Board (CCB)<br>Test coordination when external parties are involved (for example Caltrans)<br>Data collection, management and distribution (to be defined in new SOP/EOP) |
| TIC | Participation in information and requirements gathering<br>Document development and review<br>Data collection, management and distribution |
| Active Partners (Caltrans, CHP, transit agencies, etc.) | Participation in Project Meetings<br>Document Review<br>Partner System Development<br>Partner System Testing<br>Partner System Operations & Maintenance<br>Data Quality Assurance |
| Potential Partners (Private data providers, etc.) | Review of System Requirements<br>Participation in Project Meetings<br>Respond to Questions from MTC and Active Partners<br>Negotiation of Potential Project Roles and Responsibilities |

| | |
|---|---|
| Contractors (SAIC, etc.) | System Recommendation<br>System Requirements and Design<br>Central System Design and Development<br>System Testing<br>System Installation<br>System Documentation<br>System O&M<br>Participation in Change Control Board |

# Attachment 1 – Glossary

| Terms | Abbreviations | Definition |
|---|---|---|
| 511 Floodgate Manager | | See "511 Manager" |
| 511 Manager | | A web-based utility application that enables users to view and/or manage various types of pre-recorded messages that can play back at different points within the 511 phone system, such as a floodgate message at a selected menu location. |
| 511 Traffic Admin | | See "Traffic Admin Page" |
| 511 Transit CMS | | See "Transit Content Management System" |
| Application Programming Interface | API | A particular set of rules and specifications that describe an interface for the interaction with a set of functions used by components of a software system. |
| Atom Feeds | | XML language format used for web data feeds |
| Break-a-Link | B-A-L | A feature in the Congestion OI application that, by using a table of pre-defined 'critical' links, generates pre-determined alternate trips that are greater in length than the normally allowed distance of 150% of the default trip distance. BAL allows closures of critical locations (currently, only the bridges have critical links assigned) to generate alternate trips greater than 150%. |
| California Highway Patrol Computer Aided Dispatch | CHP CAD | A web-based utility application that contains detailed information about all incidents to which the California Highway Patrol responds. |
| CalTrans LCS | | See "Lane Closure System" |
| Congestion OI | | A software application that allows the 511 Traveler Information Center operators to overwrite speed data on an individual link basis and to close links. When a link is closed, a roadway closed message should play and driving times should not be given for the route which includes the broken link and an alternate route will be given if its distance is less than 150% of the default route. |
| Commercial Wholesale Web Portal | CWWP | A single portal developed by Caltrans that provides travel information for California regions in various data formats. |

| | | |
|---|---|---|
| Commercial Off The Shelf | COTS | Item that is sold in substantial quantities in commercial marketplace and available to general public |
| Enhanced Data Fusion System | EDFS | A combination of computer hardware and software systems at the TIC that communicates with other subsystems, including several interrelated applications that provide the TIC staff with the ability to enter, view, and analyze relevant traffic data, and an Internet-enabled system to receive event input from other agencies and display existing events. The data fusion system extends to and includes the interfaces with the data collection and data dissemination servers. |
| Emergency Abbreviated System for the Phone | EAS for the Phone | Two phone menu structures that are available for use during emergency situations. The regional phone EAS allows the restriction of information disseminated during an emergency in order to provide critical information to as many callers as possible. The sub-regional phone EAS allows the organization of information for a sub-regional planned event or emergency in a separate menu from the regular main menu, thus making it easier for callers to access the emergency information. |
| Emergency Abbreviated System for the website | EAS for the website | An additional webpage that summarizes emergency information in a blog format. At a minimum, the regular homepage and traffic pages are redirected to this EAS webpage during major, regional emergencies. |
| Emergency Operational Procedures | EOP | Document that defines TIC staff actions in case of emergency |
| Event | | A real world happening recorded in the EDFS to be disseminated to the public users. An Event is anything that affects transportation - traffic or transit. Examples are concert, sporting event, parade, marathon, roadway construction, weather, emergencies and incidents. Incidents are unplanned events such as traffic accident, bridge/roadway closure, transit disruption and transit delay,.. |
| Event OI | | The interface through which TIC staff enter incident or event information into the EDFS. While this interface is titled the "Event OI," TIC staff enters more than just events. |
| Floodgate | | Message played by IVR at some menu branch before accepting user input |

| | | |
|---|---|---|
| Incident | | Type of an event that describes traffic/transit incident in the system |
| Interactive Voice Response | IVR | Technology that allows a computer to interact with humans through the use of voice and DTMF telephone keypad inputs |
| Java Database Connectivity | JDBC | An API for the Java programming language that defines how a client may access a database |
| Java Messaging System | JMS | A Java Message Oriented Middleware (MOM) API for sending messages between two or more clients. |
| Lane Closure System | LCS | A web-based utility application that contains lane closure information gathered on both a daily and long-term basis by Caltrans for the entire District 4 area. |
| Lightweight Directory Access Protocol | LDAP | Protocol used for accessing and maintaining distributed directory information services |
| Open Database Connectivity | ODBC | Standard software interface for accessing database management systems |
| RSS feed | | A family of web feed formats used to publish frequently updated works in a standardized format. |
| Relational database management system | RDBMS | Database management system that is based on the relational model |
| Simple Network Manager Protocol | SNMP | Internet-standard protocol for managing devices on IP networks |
| Standard Operational Procedures | SOP | Document that defines TIC staff actions on daily basis |
| Ticker | | A scrolling banner on 511.org and several modal pages that displays breaking news, including major traffic disruptions and transit delays/disruptions |
| Ticker Admin Page | | Ticker.511.org<br><br>A web-based utility application that enables users to view and/or manage the Ticker messages for all 511 sister pages. |
| Ticker Administrative Tool | | See “Ticker Admin Page” |

| | | |
|---|---|---|
| Traveler's Information Center | TIC | The 511 operations center, collocated with Caltrans and the CHP, which collects and disseminates incident and event data through 511. |
| Traffic Admin Page | | [redacted] A web-based utility application that enables users to view and/or manage the traffic messages, breaking news and construction, on traffic.511.org |
| Traffic Management Center | TMC | Caltrans central control room in each district where operators manage traffic incidents, operate the TOS equipment in the field, manage the maintenance of the roadways and oversight of traffic control for construction projects. |
| Transit Content Management System | CMS | A web-based utility application through which TIC, MTC and transit agency staff manage Transit agency service announcements onto the Transit.511.org website. |
| Extensible Markup Language | XML | Set of rules for encoding documents in machine-readable form |